Revisiting the governance of privacy

Revisiting "The Governance of Privacy": Contemporary Policy Instruments in Global Perspective

Professor Colin J. Bennett
Department of Political Science
University of Victoria
Victoria, BC. Canada
cjb@uvic.ca
www.colinbennett.ca

Professor Charles D. Raab
Politics and International Relations
School of Social and Political Science
University of Edinburgh
Charles.Raab@ed.ac.uk
http://www.pol.ed.ac.uk/people/academic_staff/raab_charles

Acknowledgements

A first draft of this paper was delivered to the 2017 Privacy Law Scholars Conference, Berkeley California. We are grateful for the helpful comments received by several attendees at our panel session, as well as the anonymous reviewers for this journal. We are also grateful to Mr. Smith Oduro-Marfo, a PhD student at the University of Victoria for assistance with the preparation of the manuscript. Funding for this work has been provided by the Social Sciences and Humanities Council of Canada's Partnership Grant on "Big Data Surveillance".

Abstract

In the early 2000s, we surveyed and analyzed the global repertoire of policy instruments deployed to protect personal data in "The Governance of Privacy." In this article, we explore how those instruments have changed as a result of 15 years of fundamental transformations in information technologies, and the new digital economy that they have produced. We review the contemporary range of transnational, regulatory, self-regulatory and technical instruments according to the same framework, and conclude that the types of policy instrument have remained remarkably stable, even though they are now deployed on a global scale, rather than in association with particular legal or administrative traditions. While the labels remain the same, however, the conceptual foundations for their legitimation and justification are shifting as a greater emphasis on accountability, risk, ethics and the social/political value of privacy have gained purchase in the policy community. Our exercise in self-reflection demonstrates both continuity and change within the governance of privacy, and displays how we would have tackled the same research project today. As a broader case study of regulation, it also highlights the importance of going beyond the technical and instrumental labels. The change or stability of policy instruments do not take place in isolation from the wider conceptualizations that shape their meaning, purpose and effect.

Introduction

Political scientists naturally gravitate towards analyzing the exercise of power in somewhat different ways from legal scholars. As students of public, and specifically regulatory policy, we tend to begin by asking how an area of social life is governed, how problems and issues are approached by those authoritative exercises of power, and how policy instruments are designed and chosen. Taken together, each jurisdiction tends to have a repertoire of instruments, or "toolbox" from which they can choose different bundles of procedural and substantive tools. There is a long tradition of public policy literature offering typologies of instruments for policy design and implementation, and raising a host of fascinating empirical, comparative and normative questions about how policy instruments are, and should be, selected (e.g., Linder & Peters 1989; Howlett 2010; Hood 1981).

We know that the repertoire of instruments associated within a particular policy sector does vary by jurisdiction. Some tools are not considered compatible

with administrative and constitutional traditions, or the wider political culture. Policy design is not, therefore, a rational exercise whereby policy makers choose the best option from the global array of available instruments. The choice is invariably shaped by context-specific constraints, styles and legacies that may be formal and legal, but which are more often subjective, cultural and informal (Vogel 1986; Howlett, Ramesh & Perl 1995).

Less clear from the literature is how the repertoire of instruments associated with a particular policy sector may change over time, as economic, social and technological conditions evolve. One would not expect the range of instruments developed to address a particular policy problem to be stable, either nationally or internationally. But how do those instruments change, and in what respects? Under what circumstances might they combine to form a regulatory regime or system that is more than the sum of its instrumental parts? And what discursive or rhetorical frameworks help to justify the adoption of particular instruments? Those are more challenging questions, inviting some careful historical and comparative analysis within and across discrete policy sectors, defined by a common policy problem.

The protection of personal data or information privacy offers a particularly interesting candidate for such an analysis. By comparison, it is a relatively new policy issue, elevated to state and global political agendas by the rapid and widespread proliferation of information and communications technologies, and the associated concerns over a multitude of risks associated with the capture, management and dissemination of personally identifiable information (PII). As a public policy (rather than just a legal) problem, privacy protection (or data protection) originates in the 1960s (Bennett 1992). Since that time, a range of legal, self-regulatory,

transnational and technological instruments have arisen, in different mixes and with different impacts, across the globe.

We analyzed these instruments more than ten years ago in *The Governance of Privacy: Policy Instruments in Global Perspective* (2003; second edition 2006; hereafter *GoP*). The book combined conceptual and theoretical discussion of several information privacy (data protection) issues[1] with empirical analysis of regulatory institutions and practices. It used social science and public policy perspectives to stretch the boundaries of the subject beyond an understanding of statutory and constitutional law and jurisprudence. It also aimed to open what were then some relatively novel windows, by asking about the nature and social distribution of privacy, about how one would measure the effectiveness of privacy protection, and about the future of global privacy governance. In line with contemporary conceptualization in the field of public policy and political science, the term *governance* was used to indicate the mutual involvement of the state, societal and other mechanisms in any field of policy–making and implementation, and to underline that an overemphasis on what the state or the government does is likely to miss or obscure many processes and structures that contribute to policy outcomes.

Since 2006, much has changed in the real and virtual worlds in which privacy governance was implicated, in the academic world that studied them, and in the policy world that aimed to regulate them. Mobile technologies, social media, "smart" everything, drones, the quantified self, and robotics were in their infancy or in pre- or early- rollout stages of development and use. Around the turn of the millennium, cloud computing, "big data", onion routing, blockchain, the Internet of Things,

[1] Terminology differs as between, for example the USA, where 'information privacy' is used more frequently, and European countries, where 'data protection' is more common. For the sake of simplicity, we use 'information privacy' throughout the paper to embrace the family of data privacy and data protection policy instruments in these countries and elsewhere.

predictive policing, and cyber-security had either not yet been conceived or had not solidified as socio-technical processes, terms in popular parlance, or matters for regulation. Many facets of the Internet and the World Wide Web were still in the bloom of youth when the study of their governance was first conceived in the 1990s. Google and Wikipedia were still in short trousers, and Facebook and Twitter had not yet been born. In the future lay the deep and shaping influence they have since had on societies, economies, the law, and everyday human relationships, and that they are expected to continue exerting on the protection of privacy and on regulatory regimes.

The pattern of threats and risks to privacy, other human rights, and ethical or democratic values was at that time shaped by practices such as e-government, e-commerce, e-health (themselves an advance on 'i-' forms of these activities), and closed-circuit TV surveillance. "M-" or networked versions of these and other consumer and citizen technological engagements were not yet prevalent. The Snowden revelations were yet to come, and malicious hacking or data breaches were not yet as massive and problematic as they have since become. Privacy invasion and protection were very rarely front-page news. Few outside technical laboratories had heard of "big data" analytics or algorithms, or used them in the daily life of businesses, policing, or the provision of government services.

When the first edition of *GoP* was published in 2003, relatively few countries beyond Europe had passed data protection or privacy laws, or had commissioners and regulatory bodies to oversee them. The European Union (EU) Data Protection Directive (1995) had only been implemented for a few years in Member States, and the Internet Corporation for Assigned Names and numbers (ICANN) had only come into being in 1996, the Budapest Convention on Cybercrime (2001) was scarcely in being, while the International Association of Privacy Professionals (IAPP), and its

efforts to coordinate a profession of privacy professionals, was still very young. The EU General Data Protection Regulation (GDPR) was a thing of the far future.

At a conceptual level, the perception of the invasion of individual privacy as a major human-rights issue had already been counterpoised by communitarian thinking (Etzioni 1999) and by a community of critical surveillance scholars, deeply skeptical of the ability of the concept and regimes of privacy to slow the rise of the surveillance society (Lyon 1994; 2001) nor to contend with broader questions of social sorting (Lyon 2003) and panoptic discrimination (Gandy 1993). The effects of 9/11 were just being felt in the emergence of new national-security, public-safety and law-enforcement discourses undermining the claims of privacy and the importance of anonymity and confidentiality. The utopian, commerce-free luster had begun to wear off the Internet, but the dystopian slime of its dark side, the ubiquity of its commercialism, and the commodification of personal information had not yet swept the boards. In academia, conferences and networks of discourse and activity on privacy and its protection against surveillance were far fewer than they have been ever since, specialist journals and publication series were thin on the ground, and there were few courses or doctoral programs in which information privacy was foregrounded.

A decade or more of change and the increasingly pervasive and intrusive processing of personal data has seen a transformation fueled by technological change and by governmental and commercial ambitions and imperatives. Those transformations raise questions about the shelf life of our attempt to make sense of the world of policy, practice, and institutional change. It is a commonplace to say that the pace of technological change outstrips the ability of law to keep up with it. But perhaps that technological lag has also supported alternative instruments of regulation

that would be more resilient and flexible, serving the interest of rights-protection better than the law itself.

GoP became a landmark source within its field, gaining wide circulation and influence among academic researchers as well as public-policy and regulatory practitioners. Now that there is vastly more scholarly as well as policy attention given to the issues discussed in *GoP,* and in the light of the questions asked above, it seems important to evaluate its relevance to the very different circumstances of technology, societal practices, regulation and policy salience in the late 2010s. That evaluation is not only an exercise in self-reflection, it also provides a critical "then and now" perspective on key theoretical and methodological questions about the definition of policy instruments and their stability over time.

The Governance of Privacy: The Policy Instruments Approach

In *GoP*, we analyzed the variety of instruments – international, regulatory, self-regulatory, and technical – that were the most common "tools" inscribed in the policies, laws and regulatory practices of a growing number of countries. We evaluated these tools and their sub-categories with the aim of situating the armory of resources in a world of regulation that was likely to become both more global in scope and more joined-up in operation. Is our categorization still relevant to the regulatory instruments of the late 2010s? Are some of the current tools further ramifications of the original instruments? Or are they more clearly innovations that respond to novel situations in coping with new technologies, new ways of doing business, and new ways of "doing" the state?

In identifying these categories, we also saw a need to move on from conceptualizing them as discrete regulatory mechanisms – stand-alone tools in a

"toolbox", which we thought was seen as a rather inappropriate metaphor *(GoP*: pp. 207-209) – and, instead, address them as sometimes complementary and synergistic, and sometimes conflicting and disparate, components of "privacy regimes." This perspective added theoretical insight to what would otherwise have been a mechanical account of how regulation was, or could be, practiced: this law, that code, a contract, a talismanic normative declaration, some company's privacy seal, a country's commissioner, an opt-out button, or a judicial ruling. The privacy regimes comprised a number of key actors in an interdependent system embracing government policy-makers, the regulatory body, data controllers, data subjects, technology developers and providers, and privacy advocacy groups (including the media).

We leave aside the question whether our designation of actors, their performances, and their relationships was adequate; a subsequent article revisited this territory (Raab & Koops 2009). For the sake of clarity and the categorical stability of the comparative analysis, we do not attempt in this article to re-theorize the typology of instruments. The main purpose is to compare then and now and to analyze how the tools of privacy governance have, or have not, been transformed in the light of recent technological practices and other changes. Are the tools of privacy governance stable, or have they adapted, and in if so, in what ways? And what further lessons can we learn about the regulation of privacy specifically, and the analysis of regulatory instruments, more generally?

Transnational instruments

We addressed the transnational instruments (*GoP*: Ch. 4) in terms of a number of arenas that were then prominent loci for transnational activity as well as the founts of influential normative documents or regulatory pronunciations: the Council of Europe

(CoE), the Organization for Economic Co-operation and Development (OECD), the EU, Asia-Pacific Economic Cooperation (APEC), international standards organizations, and the World Trade Organization (WTO). However, the United Nations (UN) was acknowledged in only one sentence.

There was no account of transnational networks and arrangements among countries that shared a cultural, linguistic, or historical affinity or common experiences: for example, the Francophonic and Ibero-American worlds; these were dealt with later (Raab 2010). These looser structures can influence regulatory instruments through guidance and informal 'good practice' norms. But the way these subtleties might, or might have, worked out in these contexts were beyond our more straightforward and broad-brush approach to showing "what is out there" at the transnational level. The formation of these new networks and patterns of influence have become much more evident in the last ten years, as a far larger number of countries are now members of the global club of data-protecting jurisdictions.

That said, the basic transnational tools, and a global policy regime, have been relatively stable, although the EU, the OECD and the CoE have all revised and updated their main regulatory instruments in the 2010s. Most prominently, there is now the EU's General Data Protection Regulation 2016/679 (GDPR) and its data protection Directive 2016/680 regarding policing and criminal justice. The former replaced the Data Protection Directive 95/46 EC, while the latter replaced the Framework Decision 2008/977/JHA, itself a transnational instrument that postdated the publication of *GoP*. There is also the OECD-inspired Global Privacy Enforcement Network (GPEN), discussed below.

The role of international courts did not feature in *GoP* (nor did the effect of national case-law). They are now absolutely central to national and international data

protection policy, and the future interpretation of many of the GDPR's unclear provisions. Nothing like the momentous Schrems decision that invalidated the Safe Habour framework (*Schrems v. Data Protection Commissioner* 2015), or the Google Spain ruling (*Google v. AEPD* 2014) that established the so-called "right to be forgotten" would ever have been contemplated when *GoP* was written. Decisions of the ECJ and of the European Court of Human Rights (ECtHR) continue to exert a strong influence over the way laws are to be applied, over the arguments for the necessity of their revision, and over the implementation of rights across many countries.

Although the EU has been by far the most influential arena on global standards, other international arenas have emerged from the shadows in the past ten or more years. The UN has recently shown signs of greater activity, with the post-Snowden appointment in 2015 of a Special Rapporteur on the Right to Privacy and a projected program of reports stretching into the future, and with an emphasis on government surveillance. The UN's Global Pulse program ("harnessing big data for development and humanitarian action") acts within the scope of the UN's 1990 Guidelines for the Regulation of Computerized Personal Data Files, has an international advisory group, and has adopted for Global Pulse purposes a set of privacy and data protection principles that more or less copies other well-established instruments of that kind (United Nations, undated). The world's data protection commissioners have met annually since 1979, but their collective activity and interaction were barely mentioned in *GoP*; this network will be considered later.

The APEC Privacy Principles were in the process of development at the time *GoP* appeared, and were mentioned briefly. The intention was to elaborate a set of "Asian-made" standards for countries in the region, and to serve as an alternative

model for international data protection standards to that embodied in the adequacy regime of the EU. The principles themselves have not had the impact in the region that was intended. But the system of enforcement through a regime of Cross-Border Privacy Rules (CBPRs) to which companies can certify through specified and approved accountability agents is expected to be felt, as now four economies (the US, Canada, Japan and Mexico) have formally declared themselves participating economies. The APEC model represents an "organization-to-organization" approach to cross-border data regulation, in contrast to the "country-to-country" approach inherent in the EU Directive and the GDPR. Critics are still suspicious, however, that the system was designed, and currently works, to undermine the stronger enforcement of legal standards through the EU regime (Greenleaf 2014, p.34).

The international standards arena and the complex process for negotiating both technical and management standards was widely recognized at the time as a potentially valuable supplement to data protection law. In domestic and international arenas, standards could fill important gaps in the enforcement regime, relieve regulators of compliance work and serve as credible methods of certification for transnational transfers of data. The International Standards Organization (ISO), the European Committee for Standardization (CEN), the European Telecommunications Standards Institute (ETSI) and other bodies are still very active in the privacy and security realm. Perhaps the most influential have been the ISO series of 27000 security standards, including the influential ISO/EIC 27018 on the protection of personally identifiable information for cloud computing. The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) presides over a large number of processes for developing technical standards for information technology and robotics, information assurance, and other subjects. While there has thus been

extensive activity in standards organizations, the regulatory community has been somewhat slow to use standards as instruments of regulatory compliance. The world of standards setting remains often opaque, technical and complex.

Finally, we discussed the relationship between international data protection and the WTO. There had always been complaints about the economic protectionist motivations behind the tests within the 1995 EU Directive whereby third countries' data-protection provisions were assessed for their adequacy in terms of the EU's own provisions. The entire process rested on certain assumptions that these measures were indeed administered in a "reasonable, objective and impartial manner" so as not to run afoul of the non-discrimination provisions within the General Agreement on Trade in Services (GATS). We \ speculated, however, that at some point international data protection rules would be tested within the WTO; this point might be approaching because of the growing number of data-localization or residency measures, prompted in part by genuine concerns about access to personal data by US intelligence agencies, in the light of the Snowden revelations. For example, recent text for the prospective renegotiation of NAFTA suggests that US commercial and government interests align in preventing, as far as possible, "measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage of processing of data" (Malcolm 2017).

Two preliminary conclusions can be reached about the current landscape of transnational instruments and actors. The first is, of course, that once an organization enters this policy arena, it is reluctant to leave. Thus, what appeared as a mosaic of intersecting arenas of transnational governance in the mid-2000s now seems increasingly so, exacerbating issues of co-ordination and harmonization. Second, the family of international regimes was largely in this policy space before the advent of

modern, networked, global communications. The privacy issues associated with the Internet are generally not worked out within the international regimes that are responsible for Internet governance; they are resolved (or not) within regimes that predate the Internet, and that have many other policy responsibilities beyond information privacy (Murray 2007).

Regulatory Instruments

The discussion of regulatory tools in *GoP* (Ch. 5) concentrated heavily upon the general national information privacy laws that had been enacted: some 43 by the mid-2000s, most of them by European countries and a smattering elsewhere. Federal countries had also enacted sub-national legislation by this time: for example, Canada, Germany, and Australia. By the end of 2016, 120 separate legal jurisdictions had enacted information privacy laws, defined in terms of Greenleaf's (2014, p.52) criteria: a comprehensive national scope; a set of minimum data privacy principles; meeting a standard at least approximating the minimum provided for by the OECD Privacy Guidelines of 1980 and the Council of Europe Convention of 1981; and some official enforcement mechanisms. Many countries in Asia, Africa, and Latin America had joined the "club" over the previous decade or so (Greenleaf 2017), and there were others that were positioning themselves to do so. But the numbers game showing how many countries have adopted information privacy laws is less important than an acknowledgement of the growth from few to many and of their geographical spread. Important, too, is their diversity in scope, in their implementation machinery, and in their effectiveness (GoP: Ch. 9).

We do not enter into this area of quantitative analysis except to note the phenomenal growth trajectory, and to point out that such analysis has the merit of

stimulating deeper thought on a number of issues that Greenleaf (2014) identified: What is a country? What is a law? What scope must a law have? What data privacy principles must a law include? And how effective must a law be? Finding answers would reveal many similarities, and probably a continuing international policy convergence (Bennett 1992) around a common, but probably broader, set of privacy principles than was present when *GoP* originally analyzed the situation. Within the EU, the GDPR can be seen as re-converging the rules interpreting the principles following twenty or more years in which Member States' data protection had drifted somewhat apart.

A prominent feature of regulatory instruments is the data protection authorities (DPAs) or supervisory bodies – charged with overarching responsibility for regulating information privacy. DPAs have been crucial regulatory instruments and their growing importance in the future is signaled in the GDPR, as is indicated below. *GoP* disaggregated their roles into prototypical components that seemed to reflect the reality of these agencies' tasks and in terms of which their efficacy could be evaluated. With variations across them, *GoP* described DPAs as playing the roles of ombudsman, auditor, consultant, educator, negotiator, policy adviser, and enforcer. This seems still to be an accurate and well-recognized inventory, although for any DPA the resources given to each of these roles has always varied, and varies still. Recent scholarship has acknowledged this inventory, adapting it and highlighting certain roles (Bieker 2017; Barnard-Wills 2017; Hijmans 2016; Jóri 2015). The typology formed the basis of the internal self-assessment by DPAs under the 'London Initiative' of 2007-08.

There is evidence that DPAs have increased their educational activities –

raising public awareness, or providing guidance and advice for data controllers. However enforcement (order-making, sanctioning, fining) has become a more prominent role than before, depending upon the extent of a DPA's enforcement powers. Privacy Commissioners' offices that have relied on the pure ombuds role of complaints investigation and resolution rather than enforcement powers (such as in Australia and Canada) have been under increasing pressure to revise that model in recognition of the powerful institutional and technological forces that now need to be regulated. Systematic research and more fine-grained analysis would be able to describe shifts in the patterns of role-playing within and across DPAs, and to account for stability and change by examining variables such as personnel, resources, the popular salience of privacy-related issues, pressure from the media, NGOs and politicians, and changes in DPA leadership.

The effect upon DPAs of broad changes in the technological, economic and political drivers of information-processing activities is an unexplored subject in the institutional analysis of public policy; Hoofnagle's (2016) work on the US Federal Trade Commission (FTC) is an exemplary exception. For example, the prevalence of social media gives DPAs new privacy problems to handle, as well as new opportunities to raise individuals' awareness of the dangers these media pose. Major legislative changes, such as the GDPR, have highlighted the need for guidance among data controllers and processors, but have also revealed shortcomings in DPAs' ability to comprehend and keep abreast of technological change in order to guide intelligently and deploy their resources effectively (Raab & Székely 2017). These changes in the world that DPAs try to regulate are likely to explain new relationships between DPAs and companies' data protection officers (Bamberger & Mulligan 2015), who often understand what privacy and its protection means in specific

organizational settings; as well as between them and NGOs or privacy advocates, who often have a better grasp of technical developments (Bennett 2008).

The work of DPAs has, in part, expanded beyond national boundaries to the extent that they have developed more coordinated transnational activities. In addition to the need for EU authorities to co-operate under the "one-stop-shop" mechanism with regard to third countries, Chapters VI and VII and many Recitals of the GDPR provide for DPA's co-operation, consistency, and joint operation. The enhancement of EU DPAs' role may also have implications for the way non-EU DPAs act in global regulation, for which an important step was taken when the Global Privacy Enforcement Network (GPEN), embracing more than 50 national and sub-national regulatory authorities, was formed in 2010 to implement the 2007 OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy; it issued an Action Plan in 2012 (GPEN 2012).

DPAs' international visibility has also increased in terms of the creation of a welter of resolutions, declarations and initiatives at annual international conferences. These are intended to raise the profile of privacy protection on a host of topical issues including cloud computing, children's online privacy, social media, standardization, profiling, "big data", and search engines (Raab 2011, 2010). The long-established Berlin Group of regulators and experts in the telecommunications and media sector continues to meet, sharing knowledge, investigating issues, drafting working papers, and adopting resolutions (Berliner Beauftragter für Datenschutz und Informationsfreiheit 2013). Although the world's commissioners form a global arena for exerting some influence, they may only slowly be gaining the organizational capacity or jurisdictional legitimacy to be counted as a vehicle of choice for shaping

policy instruments in the same sense as do the OECD or CoE, for instance. But the forging of links beyond national boundaries and the attempts to act transnationally are perhaps an example of bottom-up internationalization, and the early stages of transnational regime-formation. The GDPR permits Member States to establish other supervisory authorities besides DPAs, and this might influence further adjustment in DPAs' roles and their alignment with other agencies' regulatory functions.

Data protection laws and regulatory policy have long relied on a now-familiar and nearly universal set of fair information principles (FIPs) or their equivalent in other international-level documents and in national laws. Compliance routines, sanctions, and commendations for good practice point to the supremacy of such principles although they might be interpreted and applied differently through varying legal enactment and enforcement. There is no shortage of guidance given by regulators, consultants and lawyers, but the traditional principles are hard to express in law and to put into practice in a consistent way across and within jurisdictions. This has led to some post-compliance thinking that "principles-based regulation" (PBR) (Black 2008; Raab 2012a) – despite its own inadequacies and paradoxes, including the bootstrapping dilemma of trust – might be a better route to follow in data protection as in, for example, financial regulation, especially in today's fast-moving, technologically fuelled surveillance environment. PBR chimes with "new governance" thinking about breadth and flexibility, going beyond laws, rules, and adjudication into the realm of principles. It is not enough to enunciate principles about data-handling and what the characteristics of the data need to be, but to focus somewhat more on contexts and norms (Nissenbaum 2010), and to address the broader canvas of political and organizational justifications for surveillance (Pounder 2008).

Self-Regulatory and Co-Regulatory Instruments

At the time of the writing of *GoP*, there was still very powerful resistance to the advent of information privacy law, especially for the private sector. Self-regulation or voluntary compliance were still forcefully advocated, especially in North America, as an alternative to government regulation. Thus it was argued that company and industry codes, and a menu of innovated techniques as well as better-understood and more settled avenues of law, would be preferable to the clumsiness and predictable obsolescence of omnibus legal regulation for information privacy that should be fended off by garlic, crucifix, and legal counsel. Economic self-interest as well as some academic analysis supported the position that the market itself would, over time, adjust to consumer demands for privacy protection, and that the overwhelming need for consumer trust in electronic commerce would lead to a gradual trading-up of standards (Laudon 1996).

Those arguments are still heard in the United States, but they are articulated with less frequency in other parts of the world for a number of reasons. First, the rapid diffusion of information privacy law has produced a pervasive legal-compliance culture within global companies, and in some cases forced them to harmonize their standards with the highest (and normally EU) standard. Second, comparative evaluations of self-regulation in this area have pointed to disappointing results, in the absence of a legal regulatory framework (Gellman & Dixon 2011). Third, as major actors improve their privacy standards, they expose and isolate the free riders in a particular sector, which leads to pressure on governments to restrict market access for those players.

Hence, the inventory of policy instruments that were once used to demonstrate voluntary compliance now tends to operate within a co-regulatory environment

(Hirsch 2011). They are means to implement and supplement privacy protection law, nationally and internationally, and to demonstrate best practice. That inventory has remained, however, quite consistent. *GoP* (Ch. 6) urged a clearer typology of self-regulatory instruments, in recognition of the imprecision of terminology and the indiscriminate way that words like "privacy policies", "codes of practice", "privacy standards" and so on, were appearing in company literature and on websites. A distinction was drawn between commitments, codes, standards and seals. It was argued that these instruments should be applied cumulatively: an organization should make a public commitment, codify it in policy, get certified by a standards body, and receive a privacy seal. This typology seems to hold up well in the abstract, even if terms like "privacy policy" are still used with great imprecision and their length and complexity typically baffle the average consumer.

The distinction between self-regulation and regulation is now, therefore, extraordinarily difficult to draw. Tools that once served a self-regulatory purpose are now embraced within national and international regulatory frameworks, and serve more to augment and implement legal rules than to stand in opposition to them. This tendency is seen most notably within the GDPR, which embraces several instruments – once identified with the self-regulatory environments of North America – within the scope of the regulatory framework. Thus codes of practice, privacy seals and standards, and data protection impact assessment (DPIA) all have their place and are to be encouraged, sometimes required, and sometimes standardized. Binding Corporate Rules (BCRs) were an instrument of the future ten to fifteen years ago, but they have now been adopted by multinational groups of companies to codify internal rules for the transfer of personal data within a group, and thus facilitate the international flow of personal data in conformity with data protection legislation. In

the APEC framework, Cross Border Privacy Rules (CBPRs) perform much the same role. But in many respects, these instruments are no more than complex codes of practice that define internal standards for personal data processing, and provide external evidence of accountability to the relevant regulator.

The co-regulatory model of privacy governance is most obviously now manifested in the update to the Safe Harbor Agreement, the EU-US Privacy Shield. Companies sign up to the agreement, and thereby commit to abide by its privacy obligations. There is no legal requirement for any company to self-certify, but once they do, they thereby accept the legal consequences of not adhering to the stated privacy commitments, and may be liable to challenge before the FTC, and to sanction and fine for non-compliance (Hoofnagle 2016).

Technical Instruments

The position of technical tools in the inventory of policy instruments was not well established ten to fifteen years ago. They were promoted and debated within academic and advocacy circles, but had not become mainstream. They were add-ons rather than credible and proven instruments that could stand alongside transnational, regulatory and self-regulatory solutions. There was still considerable suspicion that technology could be part of the solution, rather than part of the problem. Few DPAs embraced the possibility of using technical instruments to enforce laws, and few regulators had the technical ability to grasp the complexities of modern cryptographic methods and the like. Technology developers' understanding of privacy was still largely shaped by the concept and practice of computer security, leaving the full panoply of other privacy principles on one side. Some regulators as well as lawyers were apprehensive about the displacement of their legal guardianship of the rights underpinning data protection

law by mechanisms designed and deployed by specialists not steeped in a trained legal understanding of rights and their protection (Van Dijk *et al*. 2018).

The landscape of technological tools surveyed in *GoP* (Ch. 7) presented three categories of technical instruments: embedded systemic instruments, represented by Lessig's (1999) argument about the regulatory force of "code"; state policy-directed instruments, such as public-key infrastructures; and instruments for individual empowerment: those practical privacy tools that any individual could apply to encrypt their email, browse anonymously or pseudonymously and/or filter out cookies, spyware and other tracking codes. Each type is highly compatible with a governance approach to public policy-making and suggests different paradigms of regulatory theory. Each gives rise to research questions that move the spotlight away from the state to the design bench and the technical laboratory, and ultimately to the data subject, as the agent to be assigned responsibilities in the production of regulation.

Generalizations about trends within this field are notoriously difficult, but three significant shifts in the debate seem to have occurred since *GoP* appeared. First, to some extent, technical tools have become more mainstream, in the sense that most regulators would accept the logic of technical designs that minimize the capture of personal data and the dangers of identifying living individuals through intensive analysis. "Data protection by design and by default", ideas that originated from outside Europe, are now embraced by the GDPR. Under certain conditions, organizations are now required to "implement appropriate technical and organizational measures for ensuring that only personal data which are necessary for each specific purpose of the processing are processed" (Article 25(2)), and under certain conditions demonstrate compliance through an accredited certification body.

Anonymized data means data that "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" (GDPR, Recital 26). Pseudonymized data means personal data that have been processed "in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Article 4(5)). De-identified data means data so that the data controller, given such data, is "not in a position to identify the data subject" (Article 11(2)). These terms now acquire a status as policy concepts rather than just technical terms.

The "PII Problem" (Schwartz & Solove 2011) and the variable definitions of personal data in national law were certainly recognized at the time *GoP* was published, but there was little understanding of the complexity of the issues. The work of Sweeney (2000) and others was instrumental in convincing the community that the mere stripping of personal identifiers from a data set does not necessarily remove the risks of re-identification. The sophistication of contemporary re-identification science gives a false sense that data can ever be completely stripped of identifying markers (Ohm 2010). Analyzing "big data" can increase the risk of re-identification, and in some cases, inadvertently re-identify large volumes of de-identified data all at once.

Those insights have led to a richer discourse about the very definition of personally identified or identifiable data, about what de-identification, anonymization and pseudonymization mean in different contexts, and about what privacy risks they might mitigate. Their realism in practice, efficacy, and mathematical formulation is

keenly debated amongst computer scientists, statisticians and their cognate disciplines, and amongst some privacy legal scholars especially in the analysis of large datasets (Narayanan & Shmatikov 2010, Dwork 2006, Elliot *et al*. 2018). This policy-relevant debate is conducted in a rather different idiom from that used in older, non-technical literature on the meaning of 'privacy', and includes new kinds of experts.

A number of scholars have investigated the contours of personal data and proposed more refined categories and typologies (e.g. El Emam *et al*. 2016). A more granular analysis of the risks associated with different forms of identification and re-identification is now available. Thus the EU's Article 29 Data Protection Working Party (2014) proposed 'singling out', or "the possibility to isolate some or all records which identify an individual in the dataset"; 'linkability', or the "ability to link at least two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases)"; and 'inference', the "possibility to deduce, with significant probability, the value of an attribute from the values of other attributes".

Just as technical instruments are now more closely integrated with regulatory instruments, they are also now closely linked with self-regulation. As questions of identification and anonymity are now recognized in part as subtle questions of degree, they raise the issue of the appropriate standard or level, given the context and sensitivity of the data. Thus, strong de-identification protocols must be used in conjunction with a management framework that assesses the risks of re-identification, and there now are standards on de-identification, particularly in the health field (US, Health and Human Services 2012). Standards add a crucial element to the process of

de-identification, and can provide trusted confirmation, often in quantifiable terms, that risks have been mitigated.

The second development is that technical instruments now enter recent debates about "big data" analytics not just as supplements, but also as potential alternatives to the privacy framework based on notice and consent, although consent plays a large part in the GDPR. Some have argued that "big data" analytics or "data science" requires that presumption to be discarded, or at least fundamentally rewritten because the inductive power of analytics means that new purposes will and should be found for personal data, if the promise of the technology is to be realized. Mayer-Schönberger and Cukier (2013, p.173) are emphatic: "In the era of big data, however, when much of data's value is in secondary uses that may have been unimagined when the data was collected, such a mechanism to ensure privacy is no longer suitable." The US President's Council of Advisors for Science and Technology (2014, p.36) concurs, saying that "notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data". The issue is magnified in the context of the Internet of Things, where inferences about behavior and actions are easily drawn from the capture of data from objects in our possession – phones, cars, household appliances, etc. Most people remain in ignorance of the identifiers that attach to these devices and constantly emit information about their personal lives. The world of big data feeds off this unawareness and the ambiguity about what is, and what is not, PII (Bennett *et al*. 2014, pp.71-85). The business model of big data incentivizes the direct and indirect capture and retention of any data, by any technical means; whereas it was once cheaper to delete information than to retain it, the obverse is now the case (Mayer-Schönberger 2009).

The third significant shift is that decisions about the individual are increasingly made on the basis of inferences drawn about the categorical groups to which we are presumed to belong. This raises serious questions about social sorting, discrimination, false positives and false negatives. All of these are central to the study of surveillance and the risks incurred and the harms inflicted by new technologies, not only on the individual and her privacy, but also on society and social values more widely (Wright & Raab 2012, 2014). On the other hand, the legitimate processing of personal data is structured by a context in which there is an increasingly active and comprehensive assessment of risk, and the newly perceived importance of risk analysis is reflected in the GDPR, for example. There is lively debate about how those risk assessments should be conducted, including their incorporation into privacy impact assessment (PIA) or DPIA (Wright *et al*. 2014); for example, those mandated by the GDPR.

Privacy Governance and Policy Instruments Today

We began by asking whether the tools of privacy governance outlined in *GoP* are still generally valid, and in what ways they have been transformed. Firm conclusions are difficult to draw. However, the broad range of developments perhaps points to two general claims about larger shifts in the governance landscape that are worthy of further empirical analysis.

The first is that the tool *categories* themselves have remained quite stable. No wholly new category has been invented that would suggest a major reformulation in the overall typology. The tools are more widely understood and deployed, and they are more numerous and varied. But the range of regulatory, self-regulatory, co-regulatory and technical policy tools in the contemporary privacy protection armory is

still manifest and robust. These governance approaches, and the typologies they generated, still have normative and comparative value in a policy-making environment that is pervasively affected by the latest technological practice. Such generic concepts and frameworks sit above the cut and thrust of the latest debates, and the detailed twists and turns of feverish national and international policy-making.

On the other hand, it is certainly the case that the esteem in which each of the different types was held has waxed or waned in the passing years. Transnational instruments remain important and many have been refreshed in recent years. Regulatory instruments are still crucial but have been somewhat tarnished by law's inability to keep up with technological change, by definitional ambiguities, and by weaknesses in enforcement. Co-regulatory approaches are now more prominent, in part owing to a more serious approach to privacy protection undertaken by many leading data controllers, their industry associations, and their management and organizational changes that elevate privacy protection to a more prominent position. Technical instruments and their subtypes, such as their incorporation into products and the ability of individuals to configure the privacy they desire, have come greatly to the fore, and have been augmented by new means of protecting identities. In addition to this 'scorecard', new combinations and patterns of instruments are discernible, reshaping and to some extent further integrating privacy regimes beyond individual instruments and their sub-types.

Crucially, however, twenty years ago, the policy instruments were not globally understood or deployed. Rather, particular instruments were closely associated with particular national administrative and regulatory traditions. Thus, there were few PIAs in Europe, codes of practice were only apparent in a few countries (such as the

UK, New Zealand and the Netherlands), and privacy-enhancing technologies were generally considered useful add-ons that consumers and organizations could choose as they wished. Now there is a common recognition that all authorities need to make creative use of all the available tools, and that there are mutual involvements and dependencies among them; this possibility was scoped in *GoP* (Ch. 8). The GDPR not only revises the 1995 Data Protection Directive to produce a single harmonized regulation for the entire EU, it is also a more multi-faceted instrument, embracing and combining policy instruments (such as PIAs, codes of practice, privacy by design and by default) that have tended to originate in non-European jurisdictions. The GDPR is, therefore, a manifestation of the international diffusion of policy ideas and instruments. These instruments do not just supplement the law; they form an integral part of the entire regulatory scheme.

The second and larger claim is that the conceptual and theoretical underpinnings of the privacy policy instruments have been shifting in some discernible ways. Although the governing instruments seem quite resilient, the conceptual foundations of privacy governance are now quite different than they were 15 years ago. The definition and nature of policy instruments are rooted in their justifications. Thus, a superficial similarity in labels might obscure a more fundamental transformation in justification and legitimation. Our concluding section explores these conceptual shifts.

The Governance of Privacy: Shifts in Conceptualization

We used the term 'privacy paradigm' to "denote a set of assumptions about a phenomenon or area of study that generally go unquestioned *(GoP:* 4)." It included compliance with data-protection principles deriving from the Organization for

European Co-operation and Development and the Council of Europe. The paradigm was individualistic and rights-based; one clear objective was to protect the individual's right to information privacy, seen in terms of rights of correction, deletion and remedy, and access to her own data. The individual's knowledge and consent were important legitimizing requirements for data processing, and data controllers had to adhere to principles of transparency and accountability for compliance with measures that gave effect to the other principles.

We can identify four important and, to an extent, interrelated developments in regulatory conceptualization that serve to modify or extend the privacy paradigm, or at least test its resilience. One is the rise of *accountability* as a regulatory and self-regulatory philosophy and technique. A second is the (re-) discovery of *ethics* and its potential shaping of principles, rules and behavior in the processing of personal data. A third is the increased prevalence of *risk- and harm-based understandings* of privacy regulation, and their associated methodology, alongside the more *rights-based* philosophy. A fourth is the conceptualization of privacy as having a *social value* as well as being an individual right. This concluding discussion sketches these conceptual turns that have either challenged, enriched or undermined the privacy paradigm, and that serve to re-shape the configuration and application of policy instruments.

Accountability can now be considered an idea 'in good currency' (Schon 1973), and is highlighted in the GDPR with regard to compliance with data protection principles (Article 5) and to data breaches (Recital 86). An 'accountability principle' formed part of the FIPs identified in the OECD's 1980 Guidelines, and the 2013 revision of the Guidelines banked more heavily on data controllers' accountability in

terms of what a privacy management program should consist of, how it should notify regulators and data subjects in case of a data breach, and how the organization should be prepared to demonstrate the program to regulators or others who promote adherence to a code of conduct. How closely these valuable measures get to the heart of what accountability might mean in theory or practice is debatable. Moreover, it is far from clear how the disparate items that are considered by the OECD to be part of an accountability drive knit together: e.g., better data security, BCRs, trustmarks and privacy seals, and the – now defunct – EU-US Safe Harbor Framework. Nonetheless, an impetus has developed to improve data-controller accountability for the stewardship of personal data (Guagnin *et al.* (eds.) 2012; Hijmans 2016). This reflects, for example, the Madrid Resolution's (International Conference of Data Protection and Privacy Commissioners 2009) emphasis on principles like transparency and accountability that had been underemphasized and underpowered by DPAs.

An accountability approach is also the basis of documents produced by a project led by a group drawn from the worlds of business, academia, law and regulation under the auspices of the Centre for Information Policy Leadership (CIPL) (Raab 2012b, 2017; Bennett 2012). The self-regulatory provenance and tone of this endeavor is, however, accompanied by the co-regulatory involvement of regulators. Continuing developments of the accountability project illustrate the emphasis on *ethics*, and appear to move closer to a more explicitly normative or ethical approach although still within the realm of practice and management. But another shift could be necessary, moving closer to an ethical grounding for principles and thence, perhaps, to rules and laws as regulatory instruments. Or rather, if we judge current laws to be already rooted in ethical precepts, to reassert and perhaps to reformulate such norms

after decades of largely procedural and institutional measures to establish information privacy and data protection as public-policy and legal concerns.

This, in fact, has become a discernible trend in recent years, although a relevant antecedent was available in the late 1990s with the analysis of 'ethics for the new surveillance' (Marx 1998), which cast doubt on the fair information principles, and thus on the efficacy of regulatory regimes. This move came from the more general field of surveillance studies, outside the information privacy or data protection legal academic bubble and its emphasis on laws and procedural rules. Marx asked twenty-nine questions about the means, contexts and purposes of data collection, - although about half of them were not far from ones that could be answered by reference to existing data protection laws and principles. But they raised a host of issues that seemed to question the relevance of regulatory processes and instruments insofar as they insufficiently considered physical or psychological harm, the legitimacy and appropriateness of surveillance goals, and individuals' awareness of data collection (Raab 2012d). Ethical discourse has been around for a long time in information policy and practice (Moor 1985; Bynum 2015). "Information ethics", "digital ethics", "cyberethics" and other terms signal a partial shift from a focus on legal regulation to an emphasis on ethics that includes accountability and transparency (Raab 2017). A link to Marx's ethical catalogue, and to accountability as well as to risks and harms, is evident in Wright and Mordini's (2012) call for ethical impact assessment along the lines of technology assessment.

There are many illustrations of the new prevalence of ethics in the privacy, data protection, and information policy field. Perhaps most prominent is a 2015 initiative by the European Data Protection Supervisor, strongly emphasizing the value

of human dignity in data protection (European Data Protection Supervisor 2015a). He created an Ethics Advisory Group "to explore the relationships between human rights, technology, markets and business models in the 21st century from an ethical perspective, with particular attention to the implications for the rights to privacy and data protection in the digital environment" (European Data Protection Supervisor 2015b); the Group produced its report in 2018 (European Data Protection Supervisor 2018). The European Commission had established a European Group on Ethics in Science and New Technologies as long ago as 1991, but in 2017 re-launched it with new members, one of whom also sits on the EDPS Ethics Advisory Group (European Commission 2017). Elsewhere, other developments can be invoked: for example, in the UK, the formation of ethics groups for governmental use of biometrics and forensics, for digital policing, and for data science, as well as the government's development of an ethical framework for using digital sources of information in policy-making.

Whether this ethical clothing is just what comes down today's fashion catwalk, or something more robust and capable of shifting or enriching the regulatory armory, cannot be foretold, but it has also begun to find a niche in the business sector's development of accountability mechanisms. Thus the original work of the project on accountability has been taken over by the newly-formed Information Accountability Foundation (IAF)'s adopting the brand of "Big Data Ethics" in its work since 2013 (Information Accountability Foundation 2014). The project seeks a "common ethical frame based on key values", and identifies five key values for "big data" in a Unified Ethical Frame (UEF): "Beneficial, Progressive, Sustainable, Respectful, and Fair" (Information Accountability Foundation 2015a, pp. 8-10).

"Fair" refers to enhancing beneficial opportunities and protecting against risky actions; the link is rather to *risk analysis* and not to the "fair (and lawful)" of the traditional data protection principles or of classical and modern political, ethical, and legal philosophy. Two of the remaining ethical values of the UEF are in fact also issues concerning risk. "Beneficial" means that an organization must define the benefits from their data analytics and who gains from them; risks have to be balanced by benefits. "Progressive" means that the value given by the analytics must be better than if they were not used, and that less intensive, less risky processing should be used where they achieve the same gains.

From these values – although not necessarily uniquely from them – many questions are generated that, the project claims, need to be addressed. Some of these would indeed be novel for information-system practitioners: who benefits from, and who is at risk from, data analytics? How should important values and rights beyond privacy be taken into consideration? Should organizations aim to minimize the risks? How can all the interests of all who are affected by an application of data analytics be comprehended? How can beneficial opportunities be enhanced? These are serious questions that might indeed help to reposition thinking about data protection as something more than a legal compliance routine, and that might even engender a more sweeping analysis and a practically aimed critique of information and other technologies and their effects.

That said, this proposed new departure chimes with the EDPS' (2015, p. 4) call for a "big data protection ecosystem", "underpinned by ethical considerations", and featuring four tiers: future-oriented regulation of data processing and respect for the rights to privacy and to data protection; accountable controllers who determine

personal information processing; privacy conscious engineering and design of data processing products and services; and empowered individuals. We can see here the bringing together of diverse privacy instruments and actors under the aegis of an ethical approach that intends to restore human dignity, and not merely legal compliance, to a central position.

Risk analysis is now considered a key to unlocking ethical values and putting them into practice. *GoP* (Ch. 3) discussed risk at some length, but risk had already become a focus of attention in privacy protection (Raab & Bennett 1998). The notion of "sensitive data" is premised on the assumption that individuals would suffer greater damage if such data were misused than they would with other information deemed less sensitive. Some have argued that sensitivity is context-dependent, and indeed that privacy rights are better understood in the contexts in which personal information is implicated (Nissenbaum 2010). In particular, risk has always been the central element in the conduct of PIAs and in related systems of technology assessment and "responsible innovation". But with PIA, DPIA and "privacy by design and default" now spreading globally and finding a place within statutory law as well as in self- or co-regulation, the controversial precautionary principle (Vogel 2012; Sunstein 2005) and anticipatory action have spread from environmental, health, and other domains of policy to become implanted in privacy and information policy as well.

Risk and harm are written prominently across the GDPR, in which, for example, Recital 75 refers to the "risks to the rights and freedoms of natural persons"; again, note the individualistic focus. Recital 76 says: "[t]he likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be

evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk". However, whether this is an "objective" determination, leaving no room for dispute, is highly doubtful; and in any case, "subjective" perceptions of risk and harm are social facts as well, ones that politicians, policy-makers and regulators may have to heed more than the judgments of *soi-disant* technical experts.

Risk, harm, and the "risk of harm" were important parts of a major report by the RAND Europe (Robinson *et al.* 2009) in their review of the EU Data Protection Directive. Their report never mentioned rights, stating that "[t]he widely applauded principles of the Directive will remain as a useful front-end, yet will need to be backed up with a harms based back-end, in due time, in order to be able to cope with the challenge of globalization and international data flows" (Robinson *et al.* 2009, p. vi). Some scholars have devised typologies of risk. As far back as 1998, 6's (1998, pp. 37-45) examination of privacy "through the lens of risk" talks of groups of risks: of injustice, to personal control over collection of personal information, and to dignity by exposure or embarrassment, each group having many sub-categories. Solove (2008: Ch. 5) gives an extended catalogue of "harmful activities" grouped by four processes (information collection, processing, dissemination, and invasion), each with sub-categories of specific harms. Van den Hoven (2008) gives four types of harm that result from the loss of privacy: information-based harm (e.g., identity theft or fateful categorization), information inequality, informational injustice, and loss of moral autonomy.

No doubt, categories could be sliced and diced in many ways and include rights and freedoms (Wright & Raab 2014); the point is not to find an exclusive and

exhaustive list, but to recognize the claim that privacy policy can devise strategies not only to mitigate effects but to anticipate and prevent them. This perception may strongly affect the design and interrelationship of the entire array of instruments outlined in the *GoP*, and may influence the regulatory roles and strategies of DPAs. Where this leaves the rights-based paradigm of privacy and data protection, and how it relates to other understandings of the nature and purpose of data protection, needs further debate (Gellert 2015; van Dijk *et al.* 2018). Not uniquely in privacy applications of risk theory and analysis, epistemological and methodological problems are also evident (Raab 2005).

The fourth dimension, one that ethical approaches seem to be strengthening, is the conceptualization of privacy as not only an individual right or of personal value, but as a *social or public good*, such that its denial has repercussions on groups and categories of people and on society and the polity as well. We endorsed and developed this insight in *GoP*, but other surveillance scholars have been more assertive of its importance in the light of surveillance's discriminatory or social-sorting effects. Indeed, this understanding is not entirely absent amongst privacy advocates and regulators as well, although the extent to which they can embrace it is constrained by the persistence of the individualistic and rights-oriented paradigm. Yet it is possible to envisage, for example, PIAs stretching to comprehend impacts on trans-individual interests and values, as some have recently argued (Raab & Wright 2012; Wright & Raab 2012, 2014). The arrival of these forms of assessment through the GDPR may stimulate such fresh thinking beyond the existing approaches to impact assessment developed in the English-speaking world. Discourse about harms-based regulation might also tend in the direction of allowing wider values to be taken into the reckoning of harm. Indeed, recognizing the ethical importance of protecting

the dignity, as well as the legal rights, of social groups and categories might gain a purchase in regulatory practice, and give DPAs an extended scope in which to operate as protectors of rights and freedoms.

The social and political values of privacy seem well established in the scholarly world (e.g., Regan 1995, Solove 2008, and literature canvassed in Raab 2012c), and perhaps needs little emphasis here. But the extent to which it has traction in the practical world of lawmaking, jurisprudence, administration and regulation can be doubted, for they seem – perhaps inescapably – wedded to the conventional paradigm and can rarely see ways of stretching the concept of privacy and what needs to be protected beyond existing routines, guidance, legal compliance, and practical management. The GDPR mentions the phrase "social disadvantage" only once (Recital 75) and does not address this point. The "data subject" is, implicitly, just that: not a member of a group or a category sharing collective privacy interests that can be defended and pursued as such; class actions on her behalf are very rare in this field, although Article 80 and Recital 142 of the GDPR open an avenue to the representation of an individual complainant by a not-for-profit organization even without the individual's mandate to the organization to do so. She has rights, of course; but the social and political importance of exercising those rights seems equally undervalued, although not, it seems, in countries with current or former authoritarian or totalitarian governments, where it is highly prized. Thus, we are left with what seems a continuing bifurcation of understandings, and this will be problematic in privacy and data protection for some time to come.

In Conclusion

The privacy paradigm that framed the nature of information privacy and its

regulation, and underpinned legislation and its implementation, was based on a conception of privacy as an individual human right. It shaped the landscape for protection in terms of the basic principles outlined in leading documents such as the 1980 OECD Guidelines and the 1981 CoE Convention. It enjoined data controllers to fulfill certain obligations and gave rights to data subjects that could form the basis for complaints to DPAs and ultimately for litigation. The context for the paradigm was a much simpler information environment than has evolved since the 1980s. It was one in which individuals as citizens and consumers could realistically aspire to "informational self-determination", although in most cases that aspiration remained a forlorn hope.

The array of new conceptual departures that have come into view since the appearance of *GoP* seems to attest to some dissatisfaction with the premises and/or the incompleteness of the paradigm. Deficiencies in the implementation of accountability; the underdevelopment of risk as a major concept of relevance; the ethical implications of data processing and surveillance that go beyond the reach of the law; and the failure of conventional approaches to come to grips with trans-individual values that are affected by digital phenomena, all seem to have given rise to fresh thinking and practical innovation.

Although the privacy paradigm has not been fundamentally discredited, there are arguably rifts and tensions represented by some profound debates about risk, accountability, ethics and the social value of privacy. There is also a broader political, ethical, and social-policy discourse about state surveillance and the central role that privacy plays in a democratic society that overshadows the more particular and pragmatic search for more effective and efficient policy tools and regulatory

relationships that would fulfill the classical aims of protecting personal information.

A related implication of the proliferation of different policy instruments around the world is that distinctions between regulatory and self-regulatory modes of privacy protection are now far more different to draw. As we noted, the repertoire of instruments is now globally, rather than nationally, defined. It could even be hypothesized that the governance of privacy everywhere is now based on a co-regulatory model in which regulators give organizations advice and guidance about how and when to deploy tools, and stand in the background ready to enforce and sanction, if necessary. Organizations, for their part, are expected to demonstrate a capacity to comply with law, so that if they are investigated they can point to the DPIA, the code of practice, the care and attention of company management, the anonymization mechanisms, and perhaps the external certification, as evidence of due diligence.

For scholars of public policy and regulatory governance, the broader lessons of our analysis suggest that policy instruments should never be unhinged from their conceptual and theoretical underpinnings. Questions about the change or stability of policy instruments does not take place in isolation from the wider perspectives that give meaning and purpose to the shaping and choice of these tools. But these conceptual shifts do not all pull in the same direction, and some of them might even threaten to cast aside long-standing and totemic principles that are engrained in the privacy and data protection systems that have proliferated for the past fifty years or more.

An organizational code of practice, for example, can operate as a very different policy instrument depending on whether it is regarded as a tool of

accountability, a strategy to mitigate risk, or a way to generate a more ethical sensibility among employees. An encryption tool, likewise, fulfils different functions in a privacy regime depending on whether it advances an individual right to privacy, or a social justification of good computing practice. Even a data protection law is going to operate differently depending on whether it was passed to satisfy international trade-related concerns, to legitimate governmental IT projects or, in a genuine concern to protect the privacy of citizens. In its more instrumental view of privacy governance, *GoP*, if anything, was insensitive to the deeper and different questions of legitimation and justification that attend the choice of policy instruments by individuals and organizations alike.

What is also evident is that debates about privacy protection now play out on a broader stage of human values and rights, and of the development of technologies and information practices that threaten them. How debates about privacy protection are resolved now has far greater implications for the future of global communications and the flow of personal data, and for the very essence of the Internet. The stakes in the governance of privacy, and the choice of policy instruments, are now far higher – economically and politically – than they were when the *GoP* was conceived and written.

References

6 P (1998) *The Future of Privacy*. Volume 1, Demos, London.

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (European Commission, Working Paper No. 216, 0829/14/EN, 2014) [hereinafter Opinion on Anonymisation Techniques].

Bamberger K and Mulligan D (2015) *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. MIT Press, Cambridge, MA.

Barnard-Wills D (2017) The technology foresight activities of European Union data protection authorities. *Technological Forecasting & Social Change* 116: 142–150.

Bennett C (1992) *Regulating Privacy: Data Protection and Policy in Europe and the United States.* Cornell University Press, Ithaca, NY.

Bennett C (2008) *The Privacy Advocates: Resisting the Spread of Surveillance*. MIT Press, Cambridge, MA.

Bennett C (2012) The Accountability Approach and Data Protection: Assumptions and Caveats. In:, Guagnin D, Hempel L, Ilten C, Kroener I, Neyland D and Postigo H (eds.) *Managing Privacy through Accountability*, pp. 33-48. Palgrave Macmillan, London.

Bennett C and Raab C (2006) *The Governance of Privacy: Policy Instruments in Global Perspective.* 2nd ed., MIT Press, Cambridge, MA.

Bennett C and Raab C (2003) *The Governance of Privacy: Policy Instruments in Global Perspective*. Ashgate, Aldershot.

Bennett C, Haggerty K, Lyon D, and Steeves V (eds) (2014) *Transparent Lives: Surveillance in Canada*. Athabasca University Press, Athabasca.

Berliner Beauftragter für Datenschutz und Informationsfreiheit (2013*) International Documents on Data Protection in Telecommunications and Media*, 1983-2013. Berliner Beauftragter für Datenschutz und Informationsfreiheit: Berlin.

Bieker F (2017) Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice. In: Lehmann A, Whitehouse D, Fischer-Hübner S, Fritsch L, and Raab, C (eds.), *Privacy and Identity Management: Facing Up to Next Steps,* pp. 125-139. (11th IFIP WG 9.2, 9.5, 96/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School), Karlstad, Sweden August 21-26, 2016 Revised Selected Papers, Springer.

Black J (2008) *Forms and Paradoxes of Principles Based Regulation*, September 23, LSE Legal Studies Working Paper No. 13/2008

Bynum T (2015) Computer and Information Ethics. In: Zalta E (ed.) *The Stanford Encyclopedia of Philosophy* (Winter 2015 Edition), http://plato.stanford.edu/archives/win2015/entries/ethics-computer/

Dwork C (2006) Differential Privacy. *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming* (ICALP)(2), pp. 1–12.

El Emam K, Gratton E, Polonetsky J, and Arbuckle L (2016) *The Seven States of Data: When is Pseudonymous Data Not Personal Information?* https://fpf.org/wp-content/uploads/2016/05/states-v19-1.pdf

El Emam K (2008) Heuristics for De-identifying Health Data. *IEEE Security & Privacy* 6, 4.

Elliot M, O'Hara K, Raab C, O'Keefe C, Mackey E, Dibben C, Gowans H, Purdam K, and McCullagh K (2018) Functional Anonymisation: Personal Data and the Data Environment. *Computer Law & Security Review*, 34, 2: 201-224.

Etzioni A (1999) *The Limits of Privacy*. Basic Books, New York, NY.

European Commission (March, 2017) *Commission Appoints new Advisory Group on Ethics in Science and Technology* https://ec.europa.eu/research/index.cfm?pg=newsalert&year=2017&na=na-300317

European Data Protection Supervisor (2015a) *Opinion 4/2015: Towards a New Digital Ethics – Data, Dignity and Technology*.

European Data Protection Supervisor (2015b) *Terms of Reference for the Ethics Advisory Group set up by the EDPS on the ethical dimensions of data protection*, at https://edps.europa.eu/sites/edp/files/publication/15-12-03_termsofreference_ethics_en.pdf

European Data Protection Supervisor (2018) *Ethics Advisory Group – Report 2018*

Gandy O (1993) *Panoptic Sort: Apolitical Economy of Personal Information*. Westview Press, Boulder, CO.

Gellert R (2015) Data protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative. *International Data Privacy Law* 5, 1: 3-19.

Gellman R and Dixon P (2011) Many Failures: A Brief History of Privacy Self-Regulation in the United States, *World Privacy Forum*, at: http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf

Global Privacy Enforcement Network (GPEN) (2012) *Action Plan for the Global Enforcement Network*, at https://www.privacyenforcement.net/public/activities

Greenleaf G (2014) *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford University Press, Oxford.

Greenleaf G (2017) Countries with Data Privacy Laws and Human Rights Perspectives**.** 146 *Privacy Laws & Business International Report,* 18

Guagnin D, Hempel L, Ilten C, Kroener I, Neyland D, and Postigo H (eds.) (2012) *Managing Privacy through Accountability.* Palgrave Macmillan, London.

Hijmans H (2016) *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*. Springer, Berlin, Heidelberg, New York, NY.

Hirsch D (2011) The Law and Policy of Online Privacy: Regulation, Self-Regulation or Co-Regulation. *Seattle University Law Review* 34, 439-480.

Hood C (1983) *The Tools of Government*. Macmillan, London and Basingstoke.

Hoofnagle C (2016) *Federal Trade Commission Privacy Law and Policy*. Cambridge University Press, New York, NY.

Howlett M, Ramesh M, and Perl A (1995) *Studying Public Policy: Policy Cycles and Policy Subsystems*. Oxford University Press, Toronto.

Howlett M (2010) *Designing Public Policies: Principles and Instruments*. Routledge, London.

International Conference of Data Protection and Privacy Commissioners (2009) *International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution)*, at https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf

Information Accountability Foundation (2014) A Unified Ethical Frame for Big Data Analysis, *Big Data Ethics Project*, Version 1.0, 7 October.

Information Accountability Foundation (2015) *The Information Accountability Unified Ethical Frame for Big Data Analysis – IAF Big Data Ethics Initiative*, Part A, Draft March.

Jóri A (2015) Shaping vs. applying data protection law: two core functions of data protection authorities. *International Data Privacy Law* 5, 2: 133-143.

Laudon K (1996) Markets and Privacy. *Communications of the Association for Computing Machinery*, 39: 92-104.

Lessig L (1999) *Code and Other Laws of Cyberspace*. Basic Books, New York, NY.

Linder T and Peters B. Guy (1989) Instruments of Government: Perceptions and Contexts *Journal of Public Policy,* 9,1: 35-58

Lyon D (1994) *The Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press, Minneapolis, MI.

Lyon D (2001) *Surveillance Society: Monitoring Everyday Life*. Open University Press, Buckingham.

Lyon D (2003) *Surveillance After September 11*. Polity Press, Cambridge.

Malcolm J (2017) NAFTA Renegotiation Will Resurrect Failed TPP Proposals, *Electronic Frontier Foundation*, March 31st, 2017 at: https://www.eff.org/deeplinks/2017/03/nafta-renegotiation-will-resurrect-failed-tpp-proposals

Marx G (1998) An Ethics for the New Surveillance. *The Information Society* 14, 3: 171-186.

Mayer-Schönberger V (2009) *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, Princeton, NJ.

Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution That Will Transform How We Live, Work and Think*. Houghton, Mifflin, Harcourt, New York.

Moor J (1985) What Is Computer Ethics? *Metaphilosophy* 16, 4: 266 – 75.

Murray A (2007) *The Regulation of Cyberspace: Control in the Online Environment*. Routledge-Cavendish, Abingdon.

Narayanan A and Shmatikov V (2010) Myths and Fallacies of 'Personally Identifiable Information'. *Communications of the ACM* 53, 6: 24-26

Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, CA.

Ohm P (2010) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization'. *UCLA Law Review* 57, 1701-1777

Pounder C (2008) Nine Principles for Assessing Whether Privacy is Protected in a Surveillance Society. *Identity in the Information Society* 1,1: 1-22.

Raab C (2005) The Future of Privacy Protection. In Mansell, R. and Collins, B. (eds.), *Trust and Crime in Information Societies*, pp. 282-318. Edward Elgar, Cheltenham.

Raab C (2010) Information Privacy: Networks of Regulation at the Subglobal Level. *Global Policy* 1, 3: 291-302.

Raab C (2011) Networks for Regulation: Privacy Commissioners in a Changing World. *Journal of Comparative Policy Analysis: Research and Practice* 13, 2: 195-213.

Raab C (2012a) Regulating Surveillance: The Importance of Principles. In: Ball K, Haggerty K, and Lyon D (eds.), *Routledge Handbook of Surveillance Studies*, pp. 377-385. Routledge, London.

Raab C (2012b) The Meaning of 'Accountability' in the Information Privacy Context'. In: Guagnin D, Hempel L, Ilten C, Kroener I, Neyland D, and Postigo H (eds.) *Managing Privacy through Accountability*, pp. 15-32. Palgrave Macmillan, London.

Raab C (2012c) Privacy, Social Values and the Public Interest. In: Busch A and Hofmann J (eds.) 'Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], *Politische Vierteljahresschrift Sonderheft* 46, pp. 129-151. Nomos Verlagsgesellschaft, Baden-Baden.

Raab C (2012d) Regulating Surveillance: The Importance of Principles. In: Ball K, Haggerty K and Lyon D (eds.), *Routledge Handbook of Surveillance Studies*, pp. 377-385. Routledge, London.

Raab C (2017) Information Privacy: Ethics and Accountability. In: Brand C, Heesen J, Kröber B, Müller U and Potthast Y (eds.), *Ethik in den Kulturen – Kulturen in der Ethik: Eine Festschrift für Regina Ammicht Quinn,* pp. 335-347. Narr Francke Attempto, Tübingen.

Raab C and Bennett C (1998) The Distribution of Privacy Risks: Who Needs Protection? *The Information Society* 14, 4: 263-274.

Raab C and Koops B-J (2009) Privacy Actors, Performances and the Future of Privacy Protection. In: Gutwirth S, Poullet Y, De Hert P, de Terwangne C and Nouwt S (eds.), *Reinventing Data Protection?* pp. 207-221. Springer: Dordrecht.

Raab C and Székely I (2017) Data Protection Authorities and Information Technology. *Computer Law & Security Review* 33, 4: 421-433.

Raab C and Wright D (2012) Surveillance: Extending the Limits of Privacy Impact Assessment. In: Wright D and De Hert P (eds.), *Privacy Impact Assessment,* pp. 363-383. Springer, Dordrecht.

Regan P (1995) *Legislating Privacy: Technology, Social Values and Public Policy*. University of North Carolina Press, Chapel Hill, NC.

Robinson N, Graux H, Botterman M, and Valeri L (2009) *Review of the European Data Protection Directive*, Rand Corporation at: http://www.rand.org/pubs/technical_reports/TR710.html

Schon D (1973) *Beyond the Stable State*. Penguin Books, Harmonsworth.

Schwartz P and Solove D (2011) The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Quarterly Review* 86, 1814-1894.

Solove D (2008) *Understanding Privacy*. Harvard University Press, Cambridge, MA.

Sunstein C (2005) *Laws of Fear: Beyond the Precautionary Principle*. Cambridge University Press, Cambridge.

Sweeney L (2000) Simple demographics often identify people uniquely. *Health (San Francisco) 671*, 1-34.

Thaler R and Sunstein C (2008) *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press, New Haven, CT.

United Nations (undated). *Global Pulse: Harnessing Big Data for Development and Humanitarian Action*. https://www.unglobalpulse.org/privacy

United States, Department of Health and Human Services (2012) *Guidance regarding methods for De-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*. HHS, Washington, DC.

United States President's Council of Advisors on Science & Technology (2014) *Big Data and Privacy: A Technological Perspective*. The White House, May 1, 2014, whitehouse.gov/bigdata

van den Hoven J (2008) Information Technology, Privacy, and the Protection of Personal Data. In: Weckert J and van den Hoven J (eds), *Information Technology and Moral Philosophy*. Cambridge University Press, Cambridge.

van Dijk N, Tanas A, Rommetveit K and Raab C (2018) Right Engineering? The Redesign of Privacy and Personal Data Protection. *International Review of Law, Computers & Technology* 32, 2: 230-256.

Vogel D (1986) *National Styles of Regulation: Environmental Policy in Great Britain and the United States*. Cornell University Press, Ithaca, NY.

Vogel D (2012) *The Politics of Precaution: Regulating Health, Safety, and Environmental Risks in Europe and the United States*. Princeton University Press, Princeton, NJ.

Wright D and Mordini E (2012) Privacy and Ethical Impact Assessment. In: Wright D, and De Hert P (eds.), *Privacy Impact Assessment*, pp. 397-418. Springer: Dordrecht.

Wright D and Raab C (2012) Constructing a Surveillance Impact Assessment. *Computer Law & Security Review* 28, 6: 613-626.

Wright D and Raab C (2014) Privacy Principles, Risks and Harms. *International Review of Law, Computers & Technology* 28, 3: 277-298.

Wright D, Wadhwa K, Lagazio M, Raab C, and Charikane E (2014) Integrating Privacy Impact Assessment in Risk Management. *International Data Privacy Law* 4, 2: 155-170.

Cases Cited

Google Spain v. Agencia Espanola de Proteccion de Datos (AEPD) C-131-12. May 13, 2014, http://curia.europa.eu/juris/liste.jsf?num=C-131/12

Schrems v. Data Protection Commissioner Case C-362/14, October 6, 2015. http://curia.europa.eu/juris/document/document.jsf?text=&docid=182494&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=844164